



SECS1028 - Lab 6 - systemd-journald - Linux

notée sur 17 points - 10%

à rendre pour le 17

février

Objectif du laboratoire : manipuler les logs de systemd-journald.

Crédit pour la technique de manipulation du journal : <https://unix.stackexchange.com/questions/272662/how-do-i-clear-journalctl-entries-for-a-specific-unit-only>

Ce laboratoire nécessite deux VMs Kali connectées sur le réseau interne de Virtualbox. Choisissez une VM Kali (Kali 1) et clonez-la (Kali 2). Pour ce laboratoire, Kali 1 sera la machine d'attaque, Kali 2 la cible. Sur Kali 2, activez le service sshd (commande `sudo systemctl start ssh`). **Notez ci-dessous les adresses IP des deux VMs (1 point) :**

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali2024blue)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4d:5d:52 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.5/24 brd 192.168.2.255 scope global dynamic noprefixroute eth0
        valid_lft 580sec preferred_lft 580sec
    inet6 fe80::a00:27ff:fe4d:5d52/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(kali@kali2024blue)-[~]
$
```

```

File Actions Edit View Help
(kali@kali2024blue)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e6:4e:a3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.4/24 brd 192.168.2.255 scope global dynamic noprefixroute eth0
        valid_lft 520sec preferred_lft 520sec
    inet6 fe80::a00:27ff:fee6:4ea3/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

```

```

(kali@kali2024blue)-[~]
$ ssh kali@192.168.2.4
The authenticity of host '192.168.2.4 (192.168.2.4)' can't be established.
ED25519 key fingerprint is SHA256:ER86MK6gb3afba0cErr/zm5w7Q6mDPmo3oG0ovYHa5I.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.4' (ED25519) to the list of known hosts.
kali@192.168.2.4's password:
Linux kali2024blue 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
(kali@kali2024blue)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e6:4e:a3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.4/24 brd 192.168.2.255 scope global dynamic noprefixroute eth0
        valid_lft 330sec preferred_lft 330sec
    inet6 fe80::a00:27ff:fee6:4ea3/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
(kali@kali2024blue)-[~]

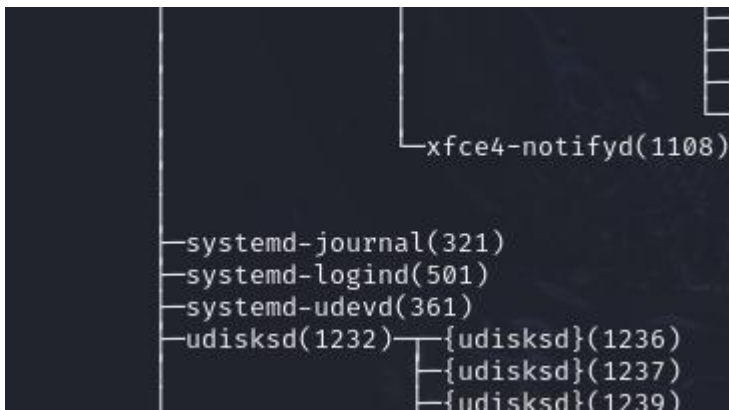
```

Vous devez ensuite utiliser uniquement la VM Kali 1 pour le laboratoire (connectée sur Kali 2 en ssh).

Vous devez insérer dans vos réponses des captures d'écran illustrant celles-ci.

1 Systemd-journald (5 points)

- 1) Sous la VM kali 1, depuis le terminal, connectez-vous sous Kali 2 en ssh. Puis, sous ssh, affichez l'arborescence des processus en cours sur Kali 2 (pstree -p). Recherchez le processus systemdjournal. Quel est son PID ? Faites une capture d'écran du PID. (1 point)



2) Sous la connexion ssh, testez la commande **journalctl -r**. Que fait-elle selon vous ? (1 point)

Elle met les plus récents logs donc les derniers logs rentrer (reverse)

```

$ journalctl -r
Feb 22 23:05:01 kali CRON[165905]: pam_unix(cron:session): session closed for user root
Feb 22 23:05:01 kali CRON[165907]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 11)
Feb 22 23:05:01 kali CRON[165905]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Feb 22 22:59:53 kali sudo[163420]: pam_unix(sudo:session): session closed for user root
Feb 22 22:59:53 kali sudo[163420]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
Feb 22 22:59:53 kali sudo[163420]:  kali : TTY=pts/1 ; PWD=/tmp ; USER=root ; COMMAND=/usr/bin/journalctl -r
Feb 22 22:58:08 kali systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Feb 22 22:58:01 kali charon[85118]: 03[KNL] flags changed for fe80::20c:29ff:fe83:682c on eth0
Feb 22 22:58:01 kali NetworkManager[748]: <info> [1740279481.2164] device (eth0): Activation: successful, devi>
Feb 22 22:58:01 kali NetworkManager[748]: <info> [1740279481.2162] manager: NetworkManager state is now CONNEC
Feb 22 22:58:01 kali NetworkManager[748]: <info> [1740279481.2161] device (eth0): state change: secondaries ->>
Feb 22 22:58:01 kali NetworkManager[748]: <info> [1740279481.2160] device (eth0): state change: ip-check -> se>
Feb 22 22:58:01 kali NetworkManager[748]: <info> [1740279481.2101] device (eth0): state change: ip-config -> i>
Feb 22 22:58:01 kali charon[85118]: 09[KNL] 192.168.3.3 appeared on eth0
Feb 22 22:58:01 kali NetworkManager[748]: <info> [1740279481.2033] dhcp4 (eth0): state changed new lease, addr>
Feb 22 22:58:01 kali NetworkManager[748]: <info> [1740279481.0074] dhcp4 (eth0): state changed new lease, addr>
Feb 22 22:57:59 kali NetworkManager[748]: <info> [1740279479.9868] dhcp4 (eth0): state changed no lease
Feb 22 22:57:59 kali charon[85118]: 16[KNL] fe80::20c:29ff:fe83:682c appeared on eth0
Feb 22 22:57:59 kali NetworkManager[748]: <info> [1740279479.9855] dhcp4 (eth0): activation: beginning transac>
Feb 22 22:57:59 kali NetworkManager[748]: <info> [1740279479.9838] device (eth0): state change: config -> ip-c>
Feb 22 22:57:59 kali NetworkManager[748]: <info> [1740279479.9830] device (eth0): state change: prepare -> con>
Feb 22 22:57:59 kali NetworkManager[748]: <info> [1740279479.9829] manager: NetworkManager state is now CONNE
Feb 22 22:57:59 kali NetworkManager[748]: <info> [1740279479.9828] device (eth0): state change: disconnected ->
Feb 22 22:57:59 kali NetworkManager[748]: <info> [1740279479.9828] device (eth0): Activation: starting connect>
Feb 22 22:57:59 kali NetworkManager[748]: <info> [1740279479.9825] policy: auto-activating connection 'Wired c>
Feb 22 22:57:59 kali NetworkManager[748]: <info> [1740279479.9809] device (eth0): state change: unavailable ->>
  
```

3) Sous la connexion ssh, affichez la date et l'heure (commande date) de la VM Kali 2. Capture l'écran. (0 point)

```

(kali@kali2024blue)-[~]
$ date
Mon Feb 10 14:19:22 AST 2025
  
```

- 4) Dans quel fichier de kali 2 est stocké l'événement que vous venez de créer (connexion SSH) ? Combien de lignes ont été créées pour cet événement ? (capture écran) (1 point)

```
Feb 10 14:26:02 kali2024blue systemd[1]: Started session-16.scope - Session 16 of User kali.  
Feb 10 14:26:02 kali2024blue systemd-logind[501]: New session 16 of user kali.  
Feb 10 14:26:02 kali2024blue sshd[31813]: pam_systemd(sshd:session): New sd-bus connection (system-bus-pam-systemd>  
Feb 10 14:26:02 kali2024blue sshd[31813]: pam_unix(sshd:session): session opened for user kali(uid=1000) by kali(u>  
Feb 10 14:26:02 kali2024blue sshd[31813]: Accepted password for kali from 192.168.2.5 port 52192 ssh2
```

1

- 5) Pouvez-vous afficher cet événement avec la commande journalctl (**journalctl -help** pour les options) et trouver sa date ? (1 point)

```
(kali) kali-[~]  
$ journalctl -u ssh.service  
Feb 22 21:53:45 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...  
Feb 22 21:53:45 kali sshd[25920]: Server listening on 0.0.0.0 port 22.  
Feb 22 21:53:45 kali sshd[25920]: Server listening on :: port 22.  
Feb 22 21:53:45 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.  
Feb 22 21:53:50 kali sshd[25966]: Connection closed by 192.168.3.8 port 43016 [preauth]  
Feb 22 21:53:55 kali sshd[26008]: Connection closed by 192.168.3.8 port 50922 [preauth]  
Feb 22 21:54:18 kali sshd[26190]: Connection closed by 192.168.3.8 port 39714 [preauth]  
Feb 22 21:54:27 kali sshd[26240]: Accepted password for kali from 192.168.3.8 port 33220 ssh2  
Feb 22 21:54:27 kali sshd[26240]: pam_unix(sshd:session): session opened for user kali(uid=1000) by kali(uid=0)  
Feb 22 21:54:27 kali sshd[26240]: pam_systemd(sshd:session): New sd-bus connection (system-bus-pam-systemd-2624>  
lines 1-10/10 (END)
```

- 6) Pouvez-vous supprimer juste la (ou les) ligne contenant cet événement dans ce fichier avec la commande journalctl ? Argumentez votre réponse. (1 point)

A l'aide d'une recherche j'ai remarqué que ce n'est pas possible de supprimer la ligne que l'on veut, l'on peut seulement supprimer à partir d'une certaine date ou sinon le fichier en entier.

2 systemd-journald - suite (8 points)

- 1) Sous la connexion ssh sur Kali 2, quelle commande permet d'afficher le nombre de logs/événements dans le journal ? (1 point)

```
(kali) kali-[~]  
$ journalctl --quiet --no-pager | wc -l  
95102  
(kali) kali-[~]
```


2) Sous la connexion ssh sur Kali 2, quelle commande permet d'exporter le journal au format texte ? Effectuez cette commande en nommant le fichier d'export "export.txt" dans le dossier /tmp de kali 2. (1 point)

```
(kali㉿ kali)-[~]
$ journalctl > /tmp/export.txt

(kali㉿ kali)-[~]
$ cd /tmp

(kali㉿ kali)-[/tmp]
$ ls
VMwareDnD
export.txt
ssh-OTvebCzzfJ5F
systemd-private-24e6dbba08cd4a40acc7b797a0f588aa-ModemManager.service-P16O5x
systemd-private-24e6dbba08cd4a40acc7b797a0f588aa-colord.service-dG6ide
systemd-private-24e6dbba08cd4a40acc7b797a0f588aa-haveged.service-H1bzsm
systemd-private-24e6dbba08cd4a40acc7b797a0f588aa-polkit.service-tMmN8G
systemd-private-24e6dbba08cd4a40acc7b797a0f588aa-systemd-logind.service-ljCxpQ
systemd-private-24e6dbba08cd4a40acc7b797a0f588aa-systemd-timesyncd.service-slAxkR
systemd-private-24e6dbba08cd4a40acc7b797a0f588aa-upower.service-tUVrfU
vmware-root_625-4021587817

(kali㉿ kali)-[/tmp]
$ |
```

3) Quelle commande permet d'exporter le journal au format texte ? Effectuez cette commande en nommant le fichier d'export "export.txt" dans le dossier /tmp. (1 point)

4) Recherchez et supprimez dans le fichier /tmp/export.txt les événements postérieurs à la date que vous avez notée. Vous vous aiderez pour cela du document suivant : https://systemd.io/JOURNAL_EXPORT_FORMATS/. (1 point)

```
(kali㉿ kali)-[~]
$ grep -B 1000 "2025-02-22" /tmp/export.txt > /tmp/nouveau_journal.txt

(kali㉿ kali)-[~]
$ mv /tmp/nouveau_journal.txt /tmp/export.txt

(kali㉿ kali)-[~]
```

5) Quelle commande permet de convertir un journal au format texte en un journal au format d'origine (binaire) ? Exécutez cette commande en nommant et plaçant le fichier de sortie dans /tmp/nouveau.journal. (1 point)

```
(kali) kali-[/tmp]
$ journalctl --file=/tmp/export.txt --output=short-precise > /tmp/nouveau.journal
Failed to open files: Bad message
```

```
(kali) kali-[/tmp]
$ ls
VMwareDnD
export.txt
hsperfdata_root
nouveau.journal
ssh-OTvebCzzfJ5F
systemd-private-24e6dbba08cd4a40acc7b797a0f588aa-ModemManager.service-OkQhO1
systemd-private-24e6dbba08cd4a40acc7b797a0f588aa-colord.service-oAdg2i
systemd-private-24e6dbba08cd4a40acc7b797a0f588aa-haveged.service-5S3R8u
systemd-private-24e6dbba08cd4a40acc7b797a0f588aa-polkit.service-Uxwt9P
systemd-private-24e6dbba08cd4a40acc7b797a0f588aa-systemd-logind.service-ljCxpQ
systemd-private-24e6dbba08cd4a40acc7b797a0f588aa-upower.service-D9XTLO
vmware-root_131811-2084452664
vmware-root_625-4021587817
```

6) Supprimez tout le contenu du journal (de kali 2) avec la commande journalctl. Quelle est cette commande ? (1 point)

```
(kali) kali-[/tmp]
$ sudo rm -rf /var/log/journal/*
```

```
(kali) kali-[/tmp]
$ sudo journalctl --rotate
sudo journalctl --vacuum-size=1K
[sudo] password for kali:
Vacuuming done, freed 0B of archived journals from /run/log/journal.
Deleted archived journal /var/log/journal/c63e5e5dd9e248ef9d74c7a81ce377c9/system@a806b41dfb0e4cc6b3921a43167e5404-0000000000017a05-00062ec60ee9a931.journal 5.2M).
Deleted archived journal /var/log/journal/c63e5e5dd9e248ef9d74c7a81ce377c9/user-1000@a806b41dfb0e4cc6b3921a43167e5404-0000000000017a0a-00062ec60ef357e0.journal 3.6M).
Vacuuming done, freed 8.9M of archived journals from /var/log/journal/c63e5e5dd9e248ef9d74c7a81ce377c9.
Vacuuming done, freed 0B of archived journals from /var/log/journal.
```

7) Remplacez le contenu du journal par le contenu du fichier /tmp/nouveau.journal. Affichez les derniers logs du journal (capture d'écran). A quelle date correspondent-ils ? (1 point)

```
(kali㉿ kali)-[/tmp]
$ sudo cp /tmp/nouveau.journal /var/log/journal/
```

8) Avec la commande journalctl, affichez les logs du journal de Kali 2 datées entre une seconde de moins et une seconde de plus que la période de la partie 1 - question 5. Obtenez 1 point si l'objectif est atteint. (1 point)

Il y a quelque chose que j'ai mal fait mais bon j'ai essayé

```
(kali㉿ kali)-[/tmp]
$ journalctl -r
Journal file /var/log/journal/nouveau.journal is truncated, ignoring file.
Feb 22 23:28:22 kali sudo[177479]: pam_unix(sudo:session): session closed for user root
Feb 22 23:28:22 kali sudo[177479]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
Feb 22 23:28:22 kali sudo[177479]: kali : TTY=pts/1 ; PWD=/tmp ; USER=root ; COMMAND=/usr/bin/cp /tmp/nouve
Feb 22 23:28:10 kali systemd[1]: NetworkManager-dispatcher.service: Deactivated successfully.
Feb 22 23:28:00 kali systemd[1]: Started NetworkManager-dispatcher.service - Network Manager Script Dispatcher >
Feb 22 23:28:00 kali dbus-daemon[716]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Feb 22 23:28:00 kali systemd[1]: Starting NetworkManager-dispatcher.service - Network Manager Script Dispatcher>
Feb 22 23:27:59 kali dbus-daemon[716]: [system] Activating via systemd: service name='org.freedesktop.nm_dispat>
Feb 22 23:27:59 kali NetworkManager[748]: <info> [1740281279.9949] dhcp4 (eth0): state changed new lease, addr>
Feb 22 23:25:01 kali CRON[175821]: pam_unix(cron:session): session closed for user root
Feb 22 23:25:01 kali CRON[175823]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)
Feb 22 23:25:01 kali CRON[175821]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)
Feb 22 23:23:15 kali sudo[174963]: pam_unix(sudo:session): session closed for user root
Feb 22 23:23:15 kali sudo[174963]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
Feb 22 23:23:15 kali sudo[174963]: kali : TTY=pts/1 ; PWD=/tmp ; USER=root ; COMMAND=/usr/bin/journalctl>--
Feb 22 23:18:30 kali sudo[172583]: pam_unix(sudo:session): session closed for user root
Feb 22 23:18:30 kali sudo[172583]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
Feb 22 23:18:30 kali sudo[172583]: kali : TTY=pts/1 ; PWD=/tmp ; USER=root ; COMMAND=/usr/bin/journalctl>--
Feb 22 23:18:30 kali sudo[172559]: pam_unix(sudo:session): session closed for user root
Feb 22 23:18:30 kali systemd-journald[57240]: Vacuuming done, freed 0B of archived journals from /var/log/journ>
```

3 Contre-mesures (3 points)

Quelle(s) contre-mesure(s) proposez-vous contre la manipulation du journal effectuée précédemment ? (3 points)

Instaurer une journalisation sécurisée, configurer le `systemd-journald` pour rendre les journaux en lecture directement après leur écriture. Stocker les journaux à distance serait aussi une bonne façon d'empêcher la modification des journaux.

Fin du laboratoire.